HOUSE OF COMMONS

Business and Trade Sub-Committee

Oral evidence: UK economic security, HC 835

Tuesday 8 July 2025

Ordered by the House of Commons to be published on 8 July 2025.

Watch the meeting

Members present: Liam Byrne (Chair); Antonia Bance; John Cooper; Sarah Edwards; Alison Griffiths; Sonia Kumar; Charlie Maynard; Gregor Poynton; Mr Joshua Reynolds; Matt Western.

Questions 164-191

Witnesses

I: Nick Folland, General Counsel, M&S, Victoria McKenzie-Gould, Corporate Affairs Director, M&S and Archie Norman, Chairman, M&S.

Examination of witnesses

Witnesses: Nick Folland, Victoria McKenzie-Gould, and Archie Norman.

Q164 **Chair:** Welcome to today's hearings of the Economic Security Sub-Committee. Our focus today is on the nation's cyber-security. We are extremely grateful to representatives from two of the country's most-loved brands coming to talk to us about some outrageous attacks that they have suffered. Archie Norman, thank you very much indeed for coming in today, and for bringing your team, Victoria and Nick, along with you. The attack that Marks & Spencer suffered was appalling. Just on a human level, it must have been extremely distressing for everyone who works at the company.

Archie Norman: Yes. I have been in and around the leadership of large British public companies for longer than I care to contemplate, with a brief interlude in this place—not a very successful one perhaps. I do not think there is anything quite like this—possibly a hostile takeover bid.

In the business world, we are used to competing and dealing with competition and customers, as well as products that do or do not work, but it is very rare to have a criminal actor in either another country or this country—we were never quite sure—seeking to stop customers shopping at M&S. They are essentially trying to destroy your business for purposes that are not entirely clear, but undoubtedly they were partly about ransom or extortion.

It was like an out-of-body experience, and I think it is fair to say that everyone at M&S experienced it. For example, our ordinary shop colleagues had to work in ways that they had not done in 30 years, and they had to work extra hours just to try to keep the show on the road. All of that aside, our tech colleagues in the cyber-team had probably no sleep, or three hours a night. It is not an overstatement to describe it as traumatic, and it has endured for some weeks. We are still in rebuild mode, and we will be for some time to come. Yes, it is like an out-of-body experience—completely extraordinary.

One thing I wanted to say is that we are very grateful for the time here. I am conscious that we have only a limited amount of time, but we want to use our experience to the benefit of not only Government but other businesses that may experience similar events. It is an open offer to you and members of the Committee to be available.

Q165 **Chair:** We are extremely grateful for that. We are conscious that a live investigation is still under way and we do not want to interfere in that in any way, but we would like to ask you a couple of questions about what happened—please be circumspect when you need to be—before we move on to the wider implications and lessons that Parliament should draw for the future, and indeed for our recommendations about the nation's economic security. You described the attack as "highly sophisticated and

targeted". Are you able to tell us who you think the attackers were and how they got in?

Archie Norman: I can give you the broad outline. First, when this happens, you do not know who the attacker is. In fact, they never send you a letter signed, "Scattered Spider". That does not happen. In fact, we did not even hear from the threat actor for approximately a week after they penetrated our systems. When this is going on, you rely completely upon your security advisers to say what they think is happening. They recognise the threat actor by the attack vector—in other words, the pattern that they use.

Remember that the attacker is also working through intermediaries. We believe that in this case there was the instigator of the attack, and also DragonForce, which is a ransomware operation we believe is based in Asia. You have loosely aligned parties working together. Does it matter who it is? Probably not. It probably does not change what you do, but it affects the psychology that you have this unknown party believed to have a peculiar name on that side of the world.

The other thing to be aware of is that the threat actor typically makes themselves known not just to us directly. As I said, that did not happen for some time, and we took an early decision that nobody at M&S would deal with the threat actor directly. We felt that the right thing was to leave this to the professionals who have experience in the matter. The threat actor also communicates through the media; in this case, they have peculiarly chosen an avenue of communication with principally, but not exclusively, the BBC. They were in contact with the BBC, and I am sure that the BBC handled it completely properly—I imagine it was in touch with law enforcement before going on air. It was an unusual experience to be brushing your teeth in the morning when someone comes on to the BBC with a communication from the people who are allegedly attacking our business.

Q166 **Chair:** Was there a ransomware demand?

Archie Norman: In almost 100% of cases there is. Part of the motivation for this is ransomware—I think that is well known—but part I do not know, because we do not know who they are. Part is probably that these are people who quite enjoy what they do. It is believed that this group are former computer gamers who graduated into cyber. That may not be true; I am relying entirely on hearsay. It is normal that some sort of ransomware demand manifests sooner or later.

As I said, we are not in a position to discuss the nature of the interaction with the threat actor. We separated our own people from that. The first time we heard from them directly was after about a week. To give some context, one of the ironies of the problem, on the business side of this, is that by the time the threat actor makes themselves evident, your systems are already compromised. One of our big pieces of learning is that once you have experienced an attack that has had any success at all, you are then in a multi-week process of systems rebuilding. Whatever you do, you

are going to have to rebuild, and it is going to take a long time to come back. That was our experience.

Q167 **Chair:** Did you have to pay the ransom demand?

Archie Norman: That is a business decision principally. The question all businesses have to ask when they look at the demand is: what are you getting for it, once your systems are compromised and you are going to have to rebuild anyway? Maybe they have exfiltrated data that you do not want them to publish, maybe there is something there, but in our case, the damage had substantially been done.

Q168 **Chair:** You had invested significantly in cyber-defences in front of this attack. You had run scenario-planning workshops to try to safeguard the business. Looking in retrospect on the preparations that you had in place, is there anything obvious that you could have done differently?

Archie Norman: In all humility, anybody who has suffered an event like ours would be foolish not to say that there are a thousand things they would like to have done differently. This has been very costly for our business, disruptive for our customers, and so on, so the answer is yes, of course there is. As you would expect, we will have an in-depth third party-facilitated review, to make sure that we have all the learning from this. We would be very happy to share that.

There have been media reports asking, "Did M&S leave the back door open?" To be clear, we didn't—that's all Horlicks. First, there is a contextual point. Businesses such as ours have a vulnerability, which is that we have a very wide attack surface, as they call it. There is all this new language you learn—the attack surface, or the perimeter. We have 50,000 people working on our systems—colleagues in the stores; contractors working for us, some may be outsourced, some may be in India—so the attack surface is enormous and the attacker, potentially, has only to be lucky once, with one of those 50,000. The right thing to do if you are in our business is to assume that the perimeter is permeable.

Ultimately, the question is: can they get in? They probably can if they try hard enough. You have all the preventions that you should have—dual-factor authentication, password control, everything like that—but there are 50,000 points of entry, so you have to assume that they can get in. In our case, the initial entry, on 17 April, occurred through what people now call social engineering. As far as I can tell, that is a euphemism for impersonation, but it was sophisticated impersonation. They didn't just rock up and say "Would you change my password?" They appeared as an individual, with their details. Part of the point of entry in our case also involved a third party. That is just a reminder that that attack surface is very hard to defend.

The second point that I would make in terms of vulnerability is that we have been around since 1884, so we do have legacy systems. Now, we probably wish that we didn't. One of the lessons is that, if you modernise your systems to be cyber-secure, they will be, but all businesses like ours have a hybrid of old and new. That hybrid makes it harder to

compartmentalise your system, so the question then is: if they get in, how easy is it to move laterally? That is inhibited by the interconnectedness of all our systems.

Part of the reason why the attack has been business-impairing for us is that we closed down the systems as part of a defence. So there was some impact, but we closed down the systems as part of the defence, which is the right thing to do. I think you will find that Co-op did the same, and probably more radically than we did. Once you have closed them down, however, bringing them back up in a safe form is very difficult.

Nick Folland: In terms of lessons learned, which I think was where the question started, something that we would say to others is: make sure that you can run your business on pen and paper, because that is what you need to be able to do for a period of time while all of your systems are down—you having taken them down yourself for protection.

Archie Norman: That is right. I talked to a chief executive of one of the banks—you may have done the same. If you are running people's payment systems and are responsible for their wages, it is true that you cannot afford to fail, so they have back-up on back-up. They have huge redundancy in their systems. That is very energy intensive—they probably have three times the cloud capacity they need—and it is a very expensive thing to do.

As a retailer, you cannot really afford to do that, so your resilience, as Nick has said, is about what you can do when your time and attendance system is not working. Well, I am old enough to remember a time when they did not work and you had clipboards instead, but you need to be ready to go back to that time, and then you improvise a way through.

Chair: That is very useful; thank you.

Q169 **Sonia Kumar:** How has the £300 million that you lost in the cyber-attack affected your future plans, and how have you changed your model? Has it changed any of your mergers or acquisitions? Has it changed any of your future plans now?

Archie Norman: That is a very good question. First, the £300 million is the estimate that we produced. That is a gross estimate of loss of profit. In other words, we will make £300 million less profit before recoveries. Recoveries might include insurance—and we expect they will—and there might be other things that we will be able to save money on during the downtime. So that figure is to give the financial market some sort of guidance, and a lot depends on how rapidly we recover from here.

Has it affected our future? Not really. Remember, the context of M&S is that, when I joined the business, it was a fairly broken business: our share price was dragging down; we made under half the profits we make today; we had £2 billion of debt; and our systems were in a pretty decrepit state. I have to say, if this had happened then, I think we would have been kippered, but we came into this year with £870 million of profit and £425 million on the balance sheet, so we were muscled up. By the way, that is

luck—well, it is also a lot of hard work, but it is fortunate that it happened now.

We strongly believe that we need to come out of this stronger. Coming out of it stronger means that we learn from the crisis. That means learning in terms of resilience, but also in terms of some of the things you do, like in the pandemic. You can do things quicker and better with less bureaucracy, so we learned from that. We will bring forward some of the rebuilding of our systems, because it makes sense to do so, and we will have to rebuild some, such as our ageing version of SAP, the core financial system, so we will bring that forward. So the result will be that our capital spending will be brought forward.

Will it change our strategy? No—in fact, it means we will put our foot down harder. We have been gaining market share for the last five years, and we have been the fastest growing food business on like-for-like sales for the last four years. We will go harder. We owe it to ourselves and to our customers to say, "We can stride on."

Q170 **Sonia Kumar:** How long do you think the rebuild time will be? What timeframe do you envision?

Archie Norman: That is one of the frustrating things. First, we all think that if your systems go down, you change the fuse and turn the lights back on, but it does not work like that, and there are several reasons for that. The straight answer to your question is that it will be months. We will still be in a form doing things with rebuilding in the months to come, but the customer will not see anything different from the end of this month—we hope it is the end of this month; it may be before that.

Remember, we have traded in all our stores fully throughout the crisis. The reason the £300 million figure is particularly impactful for us is that a third of our clothing and home business is sold online, and the online business is disabled. Roughly speaking, for each week we were not trading online, we were losing £10 million in profit. We are now up and running online, but we are not back to where we should be. Our big automated centre in Castle Donington will come back online hopefully imminently. It is a long, slow process back. We will be working to bring back or replace some of the background systems that hopefully you or customers do not see in October, November.

There are a couple of points I would make here. Once you have had one cyber-attack, you are more likely to have another—partly I suppose because you attract the attention of this community, and people see what happened. We want to make ourselves as resilient as possible for the future, and that means the way in which you bring things back has to be highly protected. Our early return was completely resilient. We had no remote working, so everybody working on systems had to be within a data centre, which was fully protected by a Juniper protection system—we call it "rings of steel". You want to come back early on in a very secure way. That takes longer than if you had multiple outsourced people working on your system from around the world.

Q171 **Gregor Poynton:** I want to ask four quick questions, hopefully with four quick answers. I will ask the same to the Co-op, because I am keen to try to get an understanding of the differences and similarities of what happened to you both and your response. You say 17 April was the date that they got in, and you found that out later. What was the date you knew that they were in?

Archie Norman: 19 April.

Q172 **Gregor Poynton:** What was the date you went public with that?

Archie Norman: We have complete details of the point and manner of entry, which we shared with the NCA, and we tracked their path through. It became evident to us in the late afternoon of the Easter Saturday—19 April—that they were in the system. We call the first crisis management team meeting that evening at 10 pm.

Q173 **Gregor Poynton:** What was the date when you shut down your site and let your customers know there was a problem?

Archie Norman: We alerted all the relevant authorities the following day or when they were back to work after Easter. That included the NCA, NCSC, the FCA, the ICO and the Irish authorities. There was a whole string of people.

Q174 **Gregor Poynton:** When did you go public?

Archie Norman: We went public on the Tuesday.

Victoria McKenzie-Gould: That is the 22nd.

Archie Norman: You raised the point that when you are dealing with all this, one of the issues is that there is a media maelstrom. We are the most public of public companies, so we are used to it—it is what we expect; we have 40 million customers to look after, and 50,000 colleagues. We expect that, but you have to deal with a lot of media at a time when you cannot necessarily answer all the questions.

Q175 **Gregor Poynton:** When you realised your site was under attack, before you went public, did you let other retailers know that it was happening? If so, what was the process for that?

Archie Norman: The process for that is through the NCSC. That is their role. I have spoken to them and I have reason to believe that that is exactly what they did. You must ask the Co-op, but I think—I hope—they would have been alerted by the NCSC. We shared all the information about the vector and manner of our attack, so that they could then alert the other retailers. They operate a sector group so that they can co-ordinate.

Q176 **Gregor Poynton:** You covered some of this with the Chair's question, but it sounds like your systems were not particularly well segregated, given the legacy systems you had in place, which allowed them to move through your system. Would that be fair to say?

Victoria McKenzie-Gould: One point I would make is that we chose to take the systems down and, even at the height of the attack, more than 50% were unaffected and protected. The chairman is absolutely right in what he says: in a business like retail, if you think about the complexity of even going to the shop and picking whatever you want at any time you want, lots of systems have to talk to each other. We have 1,000 sites, effectively—each store is a different site. But there is a difference between choosing to take systems down and them being taken down, and I think we chose to do the former, not the latter.

Archie Norman: Ideally, you would have all your systems in order, but it is not possible as a retailer to have completely watertight compartments. Then a technical question arises around the software that sits between the systems and allows access. That is different for every retailer, but when you look back on this, the foundation architecture is very important to resilience, but there is never a point in time—unless you have a completely new business—where you can design it that way, so you inherit it.

I would make one other point, because I don't want people to get the wrong impression. We were very well aware of the risk. If you look at our annual report, or at any large company's annual report, you will find that cyber-risk is listed at the top of their risks. It had the full attention of the audit and risk committee. We have trebled the number of people in our business working on cyber-security to 80 over the last two or three years and doubled the amount of expenditure. Thanks to my colleague Nick Folland, curiously, we doubled our insurance cover last year—that was prescient.

Q177 **Gregor Poynton:** My final question follows up from one the Chair asked, because I was not 100% sure about the answer you gave. Yesterday, in the House of Commons, the right hon. Member for Goole and Pocklington warned about cyber-attacks and ransomware attacks, and he said: "It has come to my attention that one such company paid a very large sum to its blackmailer recently." Can I ask whether your organisation, or you, have paid that ransom?

Archie Norman: We have said that we are not discussing any of the details of our interaction with the threat actor, including that subject, but that subject is fully shared with the NCA and the relevant authorities. There are a number of reasons for that. One is that we don't think it is in the public interest to go into that subject, partly because it is a matter of law enforcement—and, to be quite clear, we think it is a matter of live law enforcement, and we want to give people the best possible chance of pursuing that action.

Secondly, part of what the threat actor is looking for is publicity. We cannot avoid them getting publicity, because they are communicating directly through the BBC and so on, but we want to make sure that we limit the amount of oxygen they have.

Q178 **Sarah Edwards:** That perfectly segues into my question. I am interested

in your experience of the insurance cover you had—whether it was enough, what the interaction was like with your insurer and, perhaps, any of the "what if" moments and what other businesses might be able to learn from that. This is going to be a threat that all businesses need to have at the top of their risk register, and perhaps there are some questions we need to understand about the state of the insurance industry. Are you able to give us a bit of information about your experience of that?

Archie Norman: Nick Folland is better able to comment than I, but we have extensive insurance cover. Some of that has been reported, although we have not publicly disclosed the details. We fully expect to make, unsurprisingly, a significant claim and we fully expect to receive some substantial recovery, but we don't know how much. That process is likely to take 18 months.

Nick Folland: I was smiling as we started to answer questions, because I think I was probably about to turn myself into an advert for the insurance industry. I think it is very important that a plc knows that these policies are available and takes them out. As far as our interaction with our insurers is concerned, as you would expect, it has been a very engaged conversation right from day one. Perhaps we all have experience of making claims on policies in our own life—that is something that you do very much hand-in-glove with your insurer. We are in an almost daily dialogue with them. They are being very supportive, and as Archie says, I think I have got some work for a period of time keeping that an active conversation.

Q179 **Sarah Edwards:** When you took out the policy, were there any terms that suggested that, if a particular type of cyber-attack were to occur, you would not have been covered?

Nick Folland: The thing that we did do in terms of structuring the policy was that, a year previously, we took look at how that market was pricing, and we realised that we were insuring for the trivia and not for the catastrophic. So we flipped the way that we were insuring: we effectively said, "We'll take the first amount of exposure ourselves, and then we will insure for the worst-case scenario." Thanks to colleagues who made that recommendation, it turns out to have been a decent decision.

Q180 **Mr Reynolds:** What support did you receive from the Government, from law enforcement and from Government agencies?

Archie Norman: We have had quite a high level of interaction from the beginning—from the time that we first reported. I think it is fair to say that it was a little slow at the beginning. In law enforcement, we were initially referred to West Yorkshire Police, which I think was the lead agency, after which we arrived at the Met and then the NCA.

Q181 **Chair:** How long did that triaging process take?

Nick Folland: I think it was over several days, and it turned into perhaps weeks. The thing to emphasis is that it was because the situation was evolving.

Q182 **Chair:** That sounds like it was quite a frustrating process.

Nick Folland: No, I would not want to convey that at all—it was just a question of being in the right channel. Initially, you are telling people that you don't know the full extent of what has happened.

Archie Norman: Although you would have to ask them, my guess is that it is a question of scale. Once the level of attack became clear, and the fact that it was affecting other people in the industry, my guess is that it escalated to the NCA. By the way, we also had an interchange with the FBI, which was very supportive. It is understandable that the FBI are more muscled up in this zone—60% of all cyber-attacks reportedly happen in America, but they would be anyway. Our security advisers were very good at helping us with those contacts.

To address the question, we have no complaint about our interaction. I would say that the interaction tends to be a little bit one way, but that is not a criticism. In other words, we are informing them of what transpires so that they can then do their deliberations or investigations. It is then the NCSC's responsibility to make sure that the information is appropriately networked. I have talked to the NCSC about this, and I think they would agree, but I would say that the level of NCSC interchange tends to be probably more at the level of a cyber-security officer. In my view, it would help to have a little bit more of a boardroom presence. When something like this happens, it is a chief executive level of issue, and that level of interchange needs to take place. That is not a criticism; it is just saying that that is their current way of operating.

This not something that we are complaining about not having, but in some countries you would have more of a single port of call. They would say, "Right, here is your account officer"—for want of a better word. They would say, "By the way, if you want us to ride in the cab with you, we will. Would you like us to come to a cyber-crisis management meeting, give you advice and listen to what is happening, so that we gain the intelligence?" That is not our current mode, and my guess is that we are just not resourced to operate at that level.

Q183 **Mr Reynolds:** On that topic, we no doubt will want to go back to Government, and the Government want to learn from this as well. Is that two-way dialogue, where they say they will join you and be with you for the process, the kind of thing that you think Government should be implementing in the future?

Archie Norman: Yes, I do think that, and I think that that would find favour with the relevant agencies too. I think they would acknowledge that that would be useful. As you will understand, they are limited in their resources. You should raise it up. If you want a growth economy, you need to have a cyber-resilient economy so that people can say, "If I invest in the UK, I am more likely to be protected against this sort of event because they have very high standards of cyber and very high-quality advisers in good national authorities." That should be our aspiration; indeed, it is rightly referenced in the industrial strategy.

Q184 **Chair:** So making our country the safest place to do business is a competitive advantage in this world?

Archie Norman: 100%. I think that is the function of having very good authorities, very fluent interchange with the enterprise community. Remember, the front-line intelligence is typically in the businesses, not in GCHQ or wherever, although GCHQ is obviously very well informed. I think you have to recognise that it is global. These threat actors are not typically based in Surrey. They might be in Malaysia or Russia. In this case they are rumoured to be in the US and the UK, but we don't know. So you have to have an authority that is capable of networking at a global level and making a punch at that level. The other point is that it is very advantageous if in this country we have leading cyber-security experts, because we have a cyber services industry. We do have some good companies who work in this space, but as you would expect, the really big operations come out of the US.

Q185 **Alison Griffiths:** You have obviously had to become cyber experts in the last few months. I heard that there has been a lot of focus on activity since the event. You said that, as a board, you have been executing change over the last two to three years. I would argue that the reputational risk, operational shutdown, supply chain chaos and financial devastation that you have encountered have been well publicised by the cyber-security industry, particularly since covid and the change in the attack surface that that brought on. You brought in a global CISO in 2023, with a new chief architect only weeks before the attack occurred. What specific actions were you taking since 2020—not in the last couple of years—to make changes to that legacy architecture and protect yourselves much earlier against the very risks that you have now come up against?

Archie Norman: I understand the question and that is the question that we obviously ask ourselves too. The broader context is that this is a business that in multiple dimensions was—to put it politely—in recovery mode and rebuild mode, and we had limited financial capacity. From around the time you refer to—2020—we have been in a much better financial position, and we certainly are now, so we can accelerate the change. That is not an excuse. When we look back on this, in all humility, will we find things about which we would say, "We wish we had done that"? Of course we will.

We have brought on board a new team, as you referred to, including a new CTO, around two years to 18 months ago, with a new CISO prior to that. As I mentioned earlier, we muscled up the defence team. The cyber-security team is there to defend, but what they have to defend is the thrust of your question. With the benefit of hindsight, would we like to have brought forward our capital spend on technology to strengthen the architecture? Yes, we would. Remember, seven years ago we started with a business that was 80% in on-the-ground servers—in computer centres. We had something that people don't talk about now: a mainframe. You might remember those. We had an IBM mainframe that we had to migrate off. So, there was quite a lot of foundation work that had to be done before we could even worry about some of the things we wanted to worry

about. We made good progress on all of that, but with that, we had also been investing heavily in new data systems to ensure we got customer data properly marshalled and harboured. The move to online is a very big change. We have a loyalty card service. All these things absorb capital. That is not an excuse; it's just saying, "Have we been investing? Yes, we have accelerated the investment."

On lessons for us or other people, there are some basic things that people sometimes forget. In a legacy system, you have very distributed systems—multiple different places. They were installed by contractors you probably no longer use. "Mapping your systems" sounds really basic, but having an absolutely rigorous map of exactly how they all interface, what is hosted in each server and who has access to it—it sounds really elementary and it is not the fancy stuff, but it is one of the things that I would advise everybody to do.

Q186 **Alison Griffiths:** Can I go back to a slightly separate topic—the role of the board? In my view, the role of the board should be to provide the governance of the executive team. Do you feel that in the period since 2020 you were, as a board and as chair of the audit and risk committee, putting sufficient focus on cyber risk, and would you make recommendations about board governance?

Archie Norman: Look, I just think that for any business that suffered a cyber-attack to turn round and say, "We put sufficient emphasis on cyber risk," would be a hard claim to make. Do we wish we had spent more, done more? Of course we do. Would it have prevented the attack? Not necessarily, but that is not a reason for not doing it. So I don't want to sit here and say, "No, we did everything possible," because I don't believe that is the case—I don't think that is the case for any business. Did we accelerate the level of intensity of attention for focus on it and the resources allocated to it? Absolutely. Our chief executive, Stuart, said to our CISO, Steve Cottrell, 18 months ago, "If you need any resources, just let me know." If you like, the CISO team is the Elastoplast, isn't it? It is the first line of defence, but it is not the critical issue.

Chair: I am keen to move on to wider implications.

Q187 **Alison Griffiths:** Could you share some broader lessons for businesses to build cyber-resilience in future, and is there a role for Government in that?

Archie Norman: Yes. To your point on governance, I think there is a lot of focus on this. We had simulations last year, and the board or the risk committee was very fully briefed on all that sort of thing. But nothing survives the first whiff of gunshot. The simulation and the red team attacks were as nothing compared with what happens and the intensity of it. I don't think you can regulate your way to security in this space. I think there are things that Government can do, and regulatory things that Government can do, but I don't think we should see that as the solution. I do think the point you are driving at, which is to make sure boards are very fully aware and intelligent about and educated about what happens and the experience when it does happen—because it is punitive, as we

have seen—is right. I am very happy to—one or two boards have already invited me to come and see them to share our war stories, which I will certainly do. But I think the Government can play a bigger role in making sure that is socialised. My view is that the level of interchange is much better, as I said, at CISO level and within the cyber-community than it is at board level, but it is not true that boards are not interested. They are a bit like us; they are saying, "We are doing everything we can," but probably there is more they could do.

Victoria McKenzie-Gould: Alison, to your point on Government support, my chairman spoke about it very well, but there is so much activity going on in different Government Departments. Science, Innovation and Technology is leading a large part of this. The Cabinet Office is leading another section of it. The Home Office is consulting at the minute, or the consultation has closed. And you obviously have the industrial strategy and Business and Trade. I think it is a question of being able to bring that together in something that is more cohesive. I think that the UK is No. 3, behind the US and China, in terms of our capability and investment in cyber, and seeing it as an asset to the economy. That is a really strong position for us to leap from. It brings the opportunity of it together, as well as managing the risks—so you help UK plc to be more resilient but also try to grow it as a sector. Thinking about that more holistically, and therefore having a single owner across Government, would be incredibly helpful.

Archie Norman: I know that time is marching on, but in answer to your question—this is probably another oblique point—we do think that mandatory reporting is a very interesting idea. It is apparent to us that quite a large number of serious cyber-attacks never get reported to the NCSC. In fact, we have reason to believe that there have been two major cyber-attacks of large British companies in the last four months, which have gone unreported. I am not on the boards of those companies, so I don't know, but that is what we have been advised. We think that that is a big deficit in our knowledge as to what is happening. I don't think it would be regulatory overkill to say that if you have a material attack—define "material"—on a company of a certain size, you are required, within a time limit, to report it to the NCSC. That would enhance the central intelligence body in this area. It is not that there is nothing that Government can do, that's for sure.

Q188 **Chair:** Are there any further reflections on things that the Government need to do?

Archie Norman: It is a bit like Alison's point to us. In 2023, a Security Committee report highlighted that this was critical to national resilience, and it advocated proper resourcing expenditure. I am not aware that we have seen a substantial increase in Government investment since that time. You would not want to be here, after a catastrophic event in three years' time, with Alison asking you: "What was your board discussing?" It is an easy thing to say, but I think that the NCA, in particular, is probably under-resourced for the task it is trying to undertake. But I do not want to speak for them, and I do not even know what resources they have.

Q189 **Chair:** The concern that we have is that there is substantial private ownership of what is, in essence, public risk. If a number of retailers were to be taken down, all at the same time, and that was coupled with a public scare campaign on social media—for example, about shortages opening up—it is easy to foresee a situation in which there would be widespread panic. This was the scenario that Lord Sedwill put to us. Do you think that there are good spaces—or good institutions—in our country, where the private and public sectors can wargame the risks that we now confront as a country, in order to think through the economic security precautions that are going to be needed in this new age?

Archie Norman: I don't think that happens now. I am not aware of it, if it does.

Q190 **Chair:** Do you think it should?

Archie Norman: Yes, but I think it has to happen at board level. I don't think it is a technical problem. I think it has to happen from chief executive or chairman to chairman. I always think that in this country, the Government are slightly coy about the way they engage with the enterprise sector, but the Government have great convening power. If we are all invited to rock up to talk about cyber-security and national resilience, we will do so, and we will want to support. Companies such as ours, that have been through the process, can add some value. I think that that is the case.

I also make the point—which I know everybody is well aware of—that at the moment, the majority of cyber-attacks are extortion-related, and they relate not exclusively to the enterprise sector. We have seen them at the British Library and in other places. But were this to be a hostile foreign actor, seeking to do damage to the state, I think we would see very different outcomes. It is not for me to speak for the state of national infrastructure, or outsourced national infrastructure, but we know that some of it would be highly vulnerable indeed.

Q191 **Matt Western:** Good to see you again, Mr Norman. I would like to pick up on the point about your legacy systems. I think that there is a learning there, maybe, for all of us—not just in the private sector but in the public sector. You mentioned the British Library. Compared with the £300 million, which you are saying is a gross estimation of the hit to profit, would you be able to tell us confidentially—probably not now—what kind of budget cost do you need to spend on upgrading your legacy systems over last year, this year and the following year? You were saying the financial situation meant you could not do the upgrades you were looking to do on your legacy systems. Versus the £300 million, that would give us some context, because therein we need to understand what UK plc needs to do against the potential hit we might be facing.

Chair: There may even be a case, you see, for tax subsidies for that kind of thing. If we judge it to be something that is really important for our economic security going forward, then there is an argument that there is a public good.

Matt Western: There could be some fiscal incentive for businesses to focus on this.

Archie Norman: There could be an idea there. To answer your question, Matt—probably the finance director will kill me—roughly, dimensionally, we are spending about £600 million to £650 million a year on capital. That is rising every year, but we are more profitable every year so we can afford it, and we have the balance sheet. Of that, we expect in excess of £200 million—close to £250 million—to go on technology-related expenditure. Of that, probably half, or it might be £150 million, would be to legacy upgrades—I say legacy upgrades, but do not think there is no business benefit to that; there is. When it comes to modern supply chain systems or merchandise assembly systems in clothing and home, what we will install will both be more resilient and more effective for the business than what we had before.

There are some difficult things. As you will understand, SAP is the foundation architecture system and propels all our financial controls. Upgrading to a modern version of SAP has some benefits, but substantially it is a nil return investment; it is just something we have to do.

Victoria McKenzie-Gould: Looking back partly to Alison's question about investment, I think the chair was being a bit coy about what he pushed the business to do earlier on. If we cover from 2019-20 to 2024, it was just over £400 million of capex in technology, and a large part of that was on modernisation. It is massively significant in terms of the capex that the business has spent while Archie has been chair.

Nick Folland: The other thing I would add is that it is not just a financial decision, because if you talk to our CTO, she will say, "We have to keep the business operating". You cannot simply switch the business off, spend lots of money, and then turn it back on. One has to factor in that there is an ongoing need for the enterprise to run during the transition.

Archie Norman: Going back to the earlier point, this is not a solution, but one thing that has happened is now most technology investment is written off over a short period of time. I remember you would buy a system and depreciate over seven or eight years, so it did not really impact the p and l. Now, broadly speaking, you are writing off over three years, and a much higher proportion of technology investment is effectively rented software stored in the cloud, and that is expensed in-year. It eats your P and L as you spend the money. That is not wrong, by the way; that is just the way it is today. You do not get capital allowances for buying a new version of SAP.

Chair: Time is against us. Archie Norman, thank you very much indeed for taking the time to reflect on the terrible experience that M&S has been through. Good luck in getting the business fully back on its feet. Thank you very much for sharing some of the implications for public policy with us this morning. That concludes this panel.